Protecting External Objects in Predict With Natural Security

This section covers the following topics:

- Protecting Adabas Databases and Files
- Protecting DDMs
- Protecting Processing Rules
- Protecting Natural Source Programs

Protecting Adabas Databases and Files

Adabas Online Services (AOS) functions that process implemented Adabas databases and files are called by the following Predict functions:

- Incorporate Adabas file
- Compare Adabas file
- Generate Adabas file (with/without option Stop users using file)
- Administration Implemented file
  Purge Adabas file (with/without option Stop users using file)
  Refresh Adabas file (with/without option Stop users using file)

With some of the above functions not only file structures but also data itself can be deleted. To avoid accidental deletion of data and data definitions, we strongly recommend reserving the use of Predict functions executing AOS functions to a limited range of users.

Note:
The protection of Predict functions which execute AOS functions is independent from the protection defined for AOS functions in the library SYSAOS.
Knowledge of Natural Security is required to carry out the tasks described in the sections below.

Activating and Deactivating Predict/AOS Security

Protection of Adabas databases and files in Predict requires that Predict/AOS Security is activated.

- Predict/AOS Security is **activated** by executing the program NSCPRDAX in the library SYSSEC and then once calling the Modify Library function for SYSDIC.
- Predict/AOS Security is **deactivated** by executing the program NSCPRDDX in library SYSSEC and then once calling the Modify Library function for SYSDIC.

Protection of Adabas Databases and Files, Concepts

Applying AOS functions to databases or file ranges in Predict can be controlled with Predict/AOS security mechanisms. Predict/AOS use can be controlled

- for **individual** users with **user-specific** AOS security profiles,
- all users **without their own user-specific profile** with **default** AOS security profiles.

How to Restrict Use of AOS Functions in Predict

Two steps are required to restrict the use of AOS functions:

- **Step 1: Specify the Dictionary Security Administrator in Natural Security**
  A dictionary security administrator must be specified for each Adabas database to be maintained with Predict/AOS functions.
  Dictionary security administrators are defined in the Predict/AOS Security Profile screen of Natural Security. See Defining the Dictionary Security Administrator in Natural Security - Activity 1, for a detailed description.
  Dictionary security administrators can give the right to process databases (or file ranges) with AOS functions either to individual users or to all users.
  Rights are given using AOS security profiles (see step 2).
- **Step 2: Define AOS security profiles in Predict**
  AOS security profiles determine which AOS functions can be applied by users to a database or a file range.
  AOS security profiles are defined with the Predict special function Security for Adabas Online Services. See Security for Adabas Online Services in the section **Special Functions** in the **Predict Administration documentation**.
  Each profile applies to a combination of a database or file range and a Natural Security user.

Defining Default Access Rights

You may wish to specify Predict/AOS rights for all users without a user-specific profile in one profile. This can be done by defining default AOS security profiles. A default profile for a database or file range applies to all users who do not have their own profile.
To define a default AOS security profile, a default user must have been defined in the Predict/AOS Security Profile screen in Natural Security.

- **Defining a Default User**
  A default user is defined by assigning a Natural Security user or user group to the dummy database number 999 in the Predict/AOS Security Profile screen.
- **Defining a Default AOS security profile**
  By assigning a profile to the default user, the profile becomes a default profile. See Defining AOS Security Profiles in Predict - Activity 2.

Note:
The prompt "Please specify who is to be responsible for which database" in the Predict/AOS Security Profile screen is not correct when defining the default user.

Defining the Dictionary Security Administrator in Natural Security - Activity 1

A dictionary security administrator for each Adabas database must be specified in Natural Security. The user or user group defined as dictionary security administrator for a database is responsible for defining the access rights for Predict users by maintaining the AOS security profiles for that database.

Rules for Defining the Dictionary Security Administrator

- Only one dictionary security administrator can be defined for a database.
- If more than one administrator is desired, a group can be specified. Each group member can then perform AOS security tasks, using the group ID.
- The users or groups must be linked to the library SYSDIC.
  If a group is specified, each individual user in the group **must not** be linked to the library SYSDIC twice (as a member of the group and as an individual user).
- If people-protection for the library SYSDIC is changed from Y to N all links and profiles will be deleted.

Prerequisites

- Predict/AOS Security must have been activated by executing the program NSCPRDAX in the library SYSSEC.
- The library SYSDIC has to be defined people-protected. The Natural Security user defining the dictionary security administrator must have the right to modify the Natural Security definition of the library SYSDIC.

The Predict/AOS Security Profile Screen

Dictionary security administrators are specified in the Predict/AOS Security Profile screen shown below. To display this screen, proceed as follows:

1. Call the function Modify Library in Natural Security for the library SYSDIC.
2. Enter Y in the field Additional options of the Modify Library screen and
3. Select the topic User Exits in the selection window that is then displayed.

```
    02-07-31              - Predict/AOS Security Profile -           13:29:18

     Please specify who is to be responsible for which database:
     Data  DIC-Sec.     Data  DIC-Sec.     Data  DIC-Sec.     Data  DIC-Sec.
     Base  Administ.    Base  Administ.    Base  Administ.    Base  Administ.
     180__ DBSECGR_     _____ _________    _____ _________    _____ _________
     999__ DEFAULT_     _____ _________    _____ _________    _____ _________
     _____ _________    _____ _________    _____ _________    _____ _________
     _____ _________    _____ _________    _____ _________    _____ _________
     _____ _________    _____ _________    _____ _________    _____ _________
     _____ _________    _____ _________    _____ _________    _____ _________
```

Columns	Meaning
Database	Number of Adabas database to be protected. 999 can be specified as a dummy database number to define a default user. See also Defining Default Access Rights.
DIC.-Sec. Administ.	Natural Security user or user group to be dictionary security administrator for the database **or** default user to be used when defining a default AOS security profile in Predict. See Defining Default Access Rights.

In the above example a Natural Security user DBSECGR is responsible for the database 180, and the Natural Security user DEFAULT is defined as the default user.

Defining AOS Security Profiles in Predict - Activity 2

Prerequisites

- AOS security profiles for a database can only be defined by the dictionary security administrator for that database.
- AOS Security Profiles can only be defined for users and user groups that are defined in Natural Security and linked to the library SYSDIC.
  Remember: If a group is specified, each individual user in the group **must not** be linked in Natural Security to the library SYSDIC twice (as a member of the group and as an individual user).

The Security for Adabas Online Services Screen

The Security for Adabas Online Services screen is called with code S in the DDA Services / Special Functions Menu of Predict.


```
 13:38:15            *****  P R E D I C T  4.2.2  *****              2002-07-31
                   - Security for ADABAS Online Services -             DDAAOSM3


                      Code    Function
                     ------   ---------------
                       A      Add new Profile
                       D      Display Profile
                       M      Modify Profile
                       P      Purge Profile
                       S      Select Profile
                       ?      Help
                       .      Terminate
                     ------   ---------------

          Enter Code : _
            File No. : _____   To File No.:
        Data Base ID : _____
        Predict-user : ________

  or direct command:
Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
      Help  Next  Term  Last  E-el  Flip  Print Impl  Conf  S-fi  Prof  Menu
```

Parameters	
Code	Calls any of the functions Add, Display, Modify, Purge, Select profile, Help or Terminate. The different functions are described in separate sections below.
File No. ... To File No.	A profile for a file or a range of files can be defined by entering file numbers. If these fields are left blank, a profile for a database is processed. To process a profile for a single file, enter the file number in both the fields File No. and To File No.
Database ID	Number of the database.
Predict user	The profile to be processed defines the rights for this user. If a group is specified, the profile applies to each user in the group. To define a **default** AOS security profile, the Natural Security user ID/group specified as default user must be specified. See Defining Default Access Rights.

Functions for Processing AOS Security Profiles in Predict

Add/Display/Modify Profile - Codes A, D, M

For Databases

If a profile for a database is processed with Add/Display/Modify profile, the Predict functions Incorporate and Compare database are allowed, disallowed or the allow/disallow values are displayed.

For Files

Protection of the Predict functions Incorporate, Compare, Generate file and the functions Purge and Refresh file of the Administration Implemented File menu are allowed, disallowed or the allow/disallow values are displayed in a screen as shown below.


```
13:40:20           *****  P R E D I C T  4.2.2  *****              2002-07-31
                 - Security for ADABAS Online Services -             DDAAOSM5

Display Profile for Data Base: 180   File: 1     to File: 255
                PREDICT-user: ACCOUNT

      Please specify 'Y' to allow function or 'N' to disallow

            Incorporate File.....................: N
            Compare File.........................: Y
            Generate File........................: N
              - with option 'STOP USERS USING FILE': N
            Maintain implementation
              Purge..............................: N
              - with option 'STOP USERS USING FILE': N
              Refresh............................: N
              - with option 'STOP USERS USING FILE': N




 Enter-PF1---PF2---PF3---PF4---PF5---PF6---PF7---PF8---PF9---PF10--PF11--PF12---
       Help  Next  Term  Last  E-el  Flip  Print Impl  Conf  S-fi  Prof  Menu
```

Purge Profile - Code P

Additional confirmation is requested before a profile is actually purged.

Select Profiles for Databases and Files - Code S

```
 13:38:46           *****  P R E D I C T  4.2.2  *****              2002-07-31
                    - Security for ADABAS Online Services -             DDAAOSM6

                   Following profiles exist for data base 180    :
  (You may mark max. 60 profiles:  M:modify  D:display  P:purge profile)

   File    PRD-user M  File    PRD-user M  File    PRD-user M  File    PRD-user M
   ------- -------- -  ------- -------- -  ------- -------- -  ------- -------- -
           ACCOUNT  _                  _                  _                  _
   1     + DEFAULT  _                  _                  _                  _
   1     + PREDICT  _                  _                  _                  _
                    _                  _                  _                  _
```

Columns	Meaning
File	File number or the first file number of a range of files the profile applies to. A plus sign indicates a range of files (see screen above).
PRD-user	User or user group whose access rights are defined in the profile.
M	The functions Add, Display, Modify and Purge profile contained in Security for Adabas Online Services screen can be called from the selection list by entering the respective code (A, D, M, P) in the column M.

Protecting DDMs

Predict functions processing DDMs/files that are protected in Natural Security are affected by security mechanisms as described in the following sections.

Generating DDMs and/or Natural Security Definitions for DDMs

Generating DDMs is affected as follows:

- DDMs for files defined in Natural Security can only be regenerated (function Generate DDM applied to existing DDMs) by users authorized in Natural Security to modify the DDM.
- Natural Security definitions can only be generated for DDMs (function Generate DDM applied with the option Generate security set to Y) by users authorized in Natural Security to add the Natural Security definition of the file.

Countersignatures may be required in both cases, depending on the Natural Security definition of the file.

Generating DDMs via an Implementation Plan

Generate DDM tasks for files defined in Natural Security are not added to an implementation plan if the user is not authorized to modify the DDM. If countersignature is necessary, a generation task will be marked as impossible and the function MO (modify generation options) must be used to enter the countersignature.

When an implementation plan is executed, the system checks that neither the Predict file/field definition nor the Natural Security definition for this file was modified. Only in this case is the Generate DDM function performed.

Purging DDMs and/or Natural Security Definitions for DDMs

DDMs protected in Natural Security and/or Natural Security definitions for a DDM can only be purged with the function Purge implementation in the Administration Implemented File menu by users authorized in Natural Security to modify the Natural Security definition of the file.
Countersignatures may be required depending on the Natural Security definition of the file.

Incorporating / Comparing DDMs

DDMs protected in Natural Security can only be incorporated / compared by users authorized in Natural Security to modify the DDM. No countersignatures are necessary.

Incorporating NDBs

If the function Incorporate NDB replaces Predict database objects of type I, it may be necessary to delete Predict file objects of types I, J and K linked to these databases.
If DDMs have been generated from the file objects of types I, J and K, these file objects can only be purged if the user is authorized to modify the Natural Security definition of the files.

Protecting Processing Rules

Free rules can be protected with the parameters (Rule in Map Editor / Rule in SYSDIC). Predict and the Natural map editor evaluate this parameter in combination with the attribute Modifier (Natural Security user or user group) of the respective Verification object as follows

Parameters Rule in Map Editor / Rule in SYSDIC	Modifier specified	Effect
N	Yes or No	Rule is not protected.
Y	Yes	Only users specified as modifiers in the Predict verification object may change a free rule.
Y	No	Rule is not protected.
F (force)	Yes	Predict verifications must have at least one modifier. Only users specified as modifiers may change a rule.
D (disallow)	Yes or No	Free processing rules may not be modified in the map editor. Disallow is not applicable to Rule in SYSDIC.

See also the Verification attribute Modifier in the section Verification in the **Predefined Object Types in Predict documentation**.

The activation of automatic rules via GENERATE RULE is protected using the definition for PRD-Ext-Object Verification rule (RU).

All other objects of type verification are protected using the definition for PRD-Docu-Object Verification (VE).

Protecting Natural Source Programs

Some Predict functions access Natural source programs. The following sections describe how these functions are affected by security mechanisms.

Redocumenting Natural Programs

To redocument a Natural program from its source, the user must be authorized in Natural Security to work with Natural utilities in the library where the program is stored.

Countersignatures may be required depending on the Natural Security definition of the library.

Selecting Text

To copy text from a Natural program with the command SELECT in the description editor or another text editor, the user must be authorized in Natural Security to work with Natural utilities in the library where the program is stored.

Countersignatures may be required depending on the Natural Security definition of the library.

